111Equation Chapter 1 Section 1Computer and information technologies in methods of systematic analysis of prime roots of prime numbers

Vostrov G. Opiata R. Stavratii M. Scherbaniuk O.

Abstract

The distribution of the primitive roots of consecutive primes has been the subject of research of many mathematicians for decades and remains so today. Understanding the structural properties of the distributions of primitive roots can help to establish the fundamental nature of prime numbers and their connections with other mathematical concepts and concepts from the field of information technology, including information theory. An attempt was made to categorize prime numbers depending on their indices, and the distribution of these indices by prime modulo was investigated. A comparative analysis of analytical and computational methods, algorithms for constructing classes of prime numbers and estimating constants in the extended and generalized Artin's conjecture is given. Methods for studying the structures of the primitive roots of systems of primes in sets of consecutive primes and analyzing their influence on the processes of forming Artin's constants have been developed. In general, this article contains an exhaustive review of the principles of formation of primitive roots and their distribution, a study of the dependence of estimates of Artin's constants on the class of prime numbers, and highlights potential avenues for future research in this area.

Keywords: distribution of primitive roots, Artin’s constants, classes of prime numbers, distribution of indices modulo prime, distances between primitive roots

Introduction

The subject of the study will be the theory of the formation of systems of primitive roots of prime numbers, which from the algebraic point of view are the basic elements of groups Fp^*. The laws of distribution of primitive roots for any prime number *p* are not generally known on the set of numbers $1,2,3,\cdots,p-2,p-1$. At the same time, you can calculate their quantity based on the number $p-1$ using the Euler [1] function. Currently, there are no methods for obtaining information about their properties, but the recursive Fermat [1] function and modern computer technology make it technologically simple to calculate their values. However, if the prime number is large, then significant computational difficulties arise. The mathematical problems of the complexity of such calculations are presented in the monograph of the famous mathematician H. Rogers [2]. It is safe to say that without modern computer technology, the problem of calculating the set of all primitive roots cannot be solved in detail. First of all, it is necessary to take into account the fact that the process of calculating primitive roots is associated with a number of technological problems. The monograph [3] proves that there exists an infinite number of positive integers for which the conditions of Fermat's theorem hold. Such numbers are called Carmichael numbers. Technologically, such numbers can be used in the recursive Fermat function, but this does not create primitive roots. Hence, we can conclude that detailed information is needed on the distribution of primes as generators of primitive roots and the recursive sequences associated with them. If we divide the value of the recursive iterations of a prime number by its magnitude, we get a sequence of real numbers in the interval $(0,1)$ that are random with an unknown probability distribution law. The study of their probability distribution law is an important and complex problem in information theory[4]. It should be noted that Kulbak's book was not the first fundamental work on information theory. The first scientific work on information theory was done by C. Shannon [5,6] in 1948 and 1949. In the following years, he published scientific works that became the basis of modern information theory[6]. When solving any scientific problem, both theoretical and applied, it is necessary to take into account the fundamental principles of information theory.

In the works of the English mathematician, a specialist in mathematical statistics, Fisher, mathematical substantiation of the basics of information theory was made by creating a measure of the amount of information in information transmission systems through communication channels under various conditions [7]. The modern mathematical theory of information was created by Kulbak and studied in detail, and the results are presented in a monograph [4]. Later, the theory of dynamic properties of information was described on the basis of entropy [7]. Algorithms and methods of modern information theory have become the fundamental basis of modern information technologies [8,9]. Modern information technologies are directly related to almost all the problems of modern number theory and dynamical systems. The justification for this statement follows from a very well-known and simple fact. The essence of the whole range of problems in number theory is related to the simple fact that there are an infinite number of primes, but at the same time their properties have been studied only for a set of finite size. Most of the fundamental problems of number theory are related to the study of mathematical problems whose formulation is oriented to their entire set. Artin's conjecture in its generalized form depends entirely on the set of all natural numbers and the set of all primes[10]. Papers [11,12,13] substantiate the complexity of mathematical problems..

Artin's hypothesis applies exclusively to the original roots, but, as was proved in [10,14], if one does not have information about the laws of distribution of indices $ind(a,p)$, then for $d(5,1,x)$ it is impossible to clearly prove why $d(5,1,x) > d(2,1,x)$. Similarly, it would be impossible to explain why $d(2,1,x) > d(8,1,x)$, $d(2,1,x) > d(27,1,x)$, $d(2,1,x) > d(125,1,x)$,.. A considerable number of other examples can be given, primarily concerning the prime roots, and in general, the indices of primes when evaluating Artin's constants, not only for individual natural numbers a but also for systems of such numbers. If we consider Artin's problem as a fundamental problem of number theory, then the question arises of universal methods and algorithms for solving it for any number a, other than plus or minus one, and which is not a square. In the works of Artin and other authors, all efforts were focused on obtaining estimates of Artin's constants [4,5] using analytical methods.

The authors focused exclusively on creating a universal analytical [4,5] method for solving this problem. With the exception of the work of Bilharts[6], in which computational methods and algorithms were practically not used. There was a simple but critical obstacle for this, which is related to the high computational complexity of the methods and algorithms for solving this problem. Fundamental works of Ch. Hooley [8,9] became the first step in creating an analytical method for solving the problem. Works related to various forms of generalization of Artin's conjecture [7] and its transfer to algebraic number theory appeared, works related to the theory of simple ideals were published [1,2]. At the same time, Artin's conjecture remained at the same level of analysis of the methods of its solution as in the first fundamental works of a number of authors. The main problem was that all efforts were related to the development of methods for estimating Artin's constant in a quantitative, exclusively analytical form. Properties of prime numbers for which the number *a* is a primitive root, were not taken into account. In works [3,7,10], sets of consecutive prime numbers first became the basis of research methods for the formation of classes of prime numbers that correspond to certain values of the indices $ind(a,p)$. At the same time, the properties of prime numbers of certain classes of their sets were taken into account. The basis of such sets were their primitive roots and indices, their laws of distribution. The basis of such sets were their primitive roots and indices, their laws of distribution. Sets of consecutive prime numbers $[p_n, p_{n+M}]$, where *n* is the number of the smallest prime number, and *M* is their number in the given set became the basis for analyzing the processes of forming classes of primes with corresponding index values.

The basis of the technology of computer modeling of the processes of formation of classes of prime numbers and the calculation of generalized Artin constants for any number *a* different from plus or minus one on the set of prime numbers was the method of statistical evaluation. The basis of this method was the hypothesis that any set of consecutive prime numbers of a certain power $[p_n, p_{n+M}]$ contains the necessary information for forming classes of prime numbers for evaluating all necessary indices. In work [3] it was proved that if we use the recursive function of Fermat's little theorem under the condition that *M* ensures the statistical sufficiency of the sample of prime numbers, then we will always get the complete information necessary for estimating the Artin constants for classes of prime numbers. According to the hypothesis, it is believed that the evaluation efficiency does not depend on the choice of a prime number p_n provided that *M* ensures the efficiency of the statistical evaluation.

A problematic element of this method is the chosen procedure for selecting a set of prime numbers under the condition of sufficient statistics, if $M=500000$ and does not depend on the choice of p_n. Index values were calculated, which became the object of further analysis by the system of created algorithms for calculating indices and forming classes of prime numbers based on index values. It was proved that first of all it is necessary to take into account the primitive roots of prime numbers in a given set of prime numbers and to have information about their distribution laws. Until now, the laws of the distribution of primitive roots of prime numbers in the general case have not been studied. An even more difficult problem is the study of the laws of index distribution $ind(a,p)>1$.

As already mentioned, the classes of prime numbers are associated with systems of arithmetic progressions, which in turn are associated with the Elliott-Halberstam hypothesis [11,12], according to which the structures of arithmetic progressions should be consistent in terms of the values of their differences. This is explained by the fact that when a set of consecutive prime numbers $[p_n, p_{n+M}]$ is chosen and the value $a=p$ is sufficiently large relative to p_{n+M}, it is necessary to significantly increase *M*, because otherwise the estimates of $c(a,i,x)$ and properties of $F(a,i,x)$ may be incorrect with from the point of view of the properties of arithmetic progressions.

Analysis of the reduced sets of prime numbers gives rise to another problem. Each prime number *p* from this set is characterized by the value $\omega(p-1)$, which can be considered as a random number with a lognormal distribution law [13]. In this work, it is proved that when the prime number p_n increases, the mathematical expectation and variance also increase, which means that the structure of the set of consecutive prime numbers changes significantly if the increase exceeds a certain limit. It is possible that, starting from certain values of p_n, the reduced sets of consecutive prime numbers at a given value of *M* may change the properties of the set with respect to the estimated Artin constants. In this case, it is possible that it will be necessary to increase *M*.

Properties of the distribution of classes of prime numbers by the value of the indices.

Modern problems of number theory are largely related to the methods of sieve theory [1,2] and methods of their solution have been created. This observation to some extent refers to Artin's conjecture. However, in this problem, the application of the sieve method has a somewhat limited character, which is due to the stability of estimates of Artin's constants for any set of values of the number *a* on the set of all prime numbers. At this time, there is no complete information about the laws of distribution of prime numbers based on the value of $\omega(p-1)$. The Erdős-Katz theorem [11] regarding the normal distribution law of $\omega(n)$ probabilities for natural numbers cannot be applied for the following reasons. First, there is a fundamental difference between primes and natural numbers in terms of their distribution in the set of natural numbers. This is evidenced by works related to studies of the distribution of natural numbers with simple divisors of limited size [13]. In the cycle of such works, it was proved that the sieve method cannot be used to solve such problems. Secondly, when analyzing the laws of the distribution of prime numbers, it is not the value of the prime numbers that is used, but the value $\omega(p-1)$ and their properties are related to the properties of this quantity. In connection with this simple remark, when applying the sieve method, it is necessary to take into account the problems that may arise.

Note that the "stability" with accuracy to εp_n of estimates for $d(a,i,x)$ and properties of classes $R(a,i,1)$ for all possible values of the index on the sets $[p_n, p_{n+M}]$ is determined by the distribution laws of $ind(a,p)$ for any p_n on set $\{1,2,3,4,5,\ldots k-1, k, k+1,\ldots, p_n-2, p_n-1\}$. Indices can be even or odd, while their number is the same $(p_n-1)/2$. Until now, the distribution laws of both even and odd indices have not been studied in detail in the general case. Possessing knowledge about the properties of such laws is important for creating a detailed model for solving problems of Artin's conjecture. The law of distribution of odd indices is still unknown, and even more intriguing is the absence of any data regarding the law of distribution of primitive roots. If you create methods of computer modeling of the processes of class formation $R(a,i,x)$ and evaluation of $d(a,i,x)$ based on analytical methods, then information about the laws of distribution $ind(a,p)$ on reduced ordered sets of prime numbers is simply necessary.

The first serious step in proving the correctness of Artin's conjecture was made in the works of Ch. Hooley [8,9]. In these works, attention was focused exclusively on the case when $a=2$. The author in [8] gave a simple justification of the method he created in the following form. A simple criterion from index theory allows us to distinguish between prime numbers *p* for which 2 is a primitive root modulo *p*. The theory of indices shows that for $p\neq 2$ and any prime divisor *q* of $p-1$, the equation $\mu_1^q \equiv 2 \pmod p$ is valid. Note that μ is a certain number that can be calculated based on the recursive function $x(0)=1, \quad x(1)=a, \quad x(n+1)\equiv ax(n) \pmod p$ (formula (3)), which is the basis of Fermat's little theorem [1,2]. We obtain the number 2 for a certain power in the process of recursive calculations for any primitive root of a given prime number *p*. Note that when we replace the primitive root of a given prime number with another primitive root, we get a different value of μ and the number 2 is obtained as a residue modulo *p*.

The transition to another primitive root leads to the fact that we will get the residue 2 on another iteration, which means that the index, which is the degree in the recursion, again according to the theory of indices in this case is divided by a prime number q_2 that divides $p-1$ and in the general case may not coincide with q_1 and the equation $\mu_2^{q_2} \equiv 2 \pmod p$ is valid. Thus, we get a set of equations that in general do not allow us to come to the conclusion reached by the author. This case is due to the fact that in this case $ind(2,p)=m$, where *m* is a composite number. Such cases can occur frequently. In this analysis, the main role belongs to the process of recursive calculations, because only this process allows us to uniquely calculate the value of the recursion cycle $card(2,p)$. The value of the index can be calculated uniquely only using the expression:

$$ind(2,p) = (p-1)/card(2,p)$$

22* MERGEFORMAT ()

Note that in the statement of Ch. Hooley it should be about this value $ind(2,p)$ and no other. The probability of such a case is different from zero, and therefore the lack of its consideration is an inaccuracy in his conclusion. We can assume that for the number $a=2$ such inaccuracy is insignificant.

It should be noted that in this case the prime number *p* has many primitive roots. Based on a rather complicated analysis, an analytical estimate for $A(2)$ of a rather complex form was obtained.

In the monograph [9] the estimation of $A(2)$ was given in a reasonable form. The author drew attention to the simple fact given above without analyzing the given variants from the theory of prime number indices. In his opinion, $a=2$ is not a primitive root of a prime number *p* if *q* divides $p-1$ and, according to the theory of indices, when calculating for any primitive root, we will find the number *j* in the recursion of Fermat's small theorem, that the equality will be true:

$$j^q \equiv 2 \ (\mathrm{mod}\ p).$$

This fact became the basis for proving the mathematical form of Artin's constant estimation on the basis of a rather complicated mathematical method, assuming that Riemann's hypothesis in Dedekind's form is valid. In general, for arbitrary values of *a* different from 2 this method is difficult to adapt to new conditions and it will not always be correct due to the fact that when estimating Artin's constants, under certain conditions, it is necessary to take into account the influence on the estimation processes of the values of $ind(a,p)>1$ and the properties of the corresponding classes $R(a,i,x)$ of primes.

For example, for $a=5$, as proved in the work [3], it is necessary to take into account the value of a certain system of odd indices. In the case when the number *a* for a given prime number *p* is not a primitive root, it is necessary to take into account the influence of the index system and the fact that the indices can be complex numbers. Let's assume that $ind(a,p)=m$. The next step is to analyze all variants of the value of *m*. If $m=q$ and *q* is a prime number, then the further analysis can coincide with the analysis of Ch. Hooley, and in the case when *m* is not a prime number, there are many options associated with its decomposition into prime factors. At the same time, a significant number of options arise due to the fact that in this case it is impossible to simply choose one of the factors into which $m=\prod q_i^{\alpha_i}$ is decomposed. Such a choice cannot be simply made without detailed justification. Thus, the sequence

$$a^{(p-1)/q_i} \equiv 1 \ (\mathrm{mod}\ p)$$
$$when \quad m=\prod q_i^{\alpha_i} > q$$

33* MERGEFORMAT ()

cannot be clearly justified and arbitrary choices lead to errors. The above remark is another factor justifying the need to apply the method of computer modeling of the processes of formation of classes of $R(a,i,x)$ for all $ind(a,p)=1$ and estimation of constants $c(a,i,x)$.

Let's consider the dynamics of the formation of classes of prime numbers and their structure at different values of the indices in ascending order in the set of basic, in a certain interpretation, values of the number $a\in\{2,5,8,20,27,125\}$. The given values of the number *a* are conditionally called basic due to the fact that based on the number $a=2$ Artin substantiated his conjecture, and all other values are related to the maximum and minimum values of Artin's constants. Of course, this property has not yet been proven by mathematical methods. Based on our analysis, this is true.

Table 1 shows the powers of the classes of primes for indices from one to twenty, calculated for the set of consecutive primes $[p_1, p_{510^5}]$ based on the method of computer modeling of the processes of formation of classes of prime numbers using the recursive Fermat function.

Index	$R(2,i,x)$	$R(5,i,x)$	$R(8,i,x)$	$R(20,i,x)$	$R(27,i,x)$	$R(125,i,x)$
1	187111	196980	112331	197025	112185	118235
2	140325	133019	84138	132924	112362	79878
3	33188	34968	99679	34954	99718	104950
4	23349	33156	14016	33172	0	19869
5	9419	0	5672	0	5653	0
6	24969	23639	74759	23551	49921	70806
7	4457	4700	2677	4718	2692	2755
8	17468	8385	10429	8227	0	5623
9	3675	3834	11050	3845	11047	11667
10	7144	14058	4430	14185	5591	8441
11	1650	1838	1025	1747	1067	1116
12	4131	5935	12460	5960	37323	17731
13	1219	1229	714	1270	700	734
14	3304	3100	239	3116	2670	1872
15	1684	0	5002	0	5642	0
16	4397	2145	2604	2059	0	1284
17	2733	736	418	725	441	491
18	2733	2634	8392	2601	4473	7969
19	551	579	333	612	313	364
20	1246	3570	742	3538	0	2152

Table 1. Dynamics of changes in the structure of classes of prime numbers

If we divide all of the values by 500000, we get Artin’s constants. The classes $R(5,i,x)$ and $R(20,i,x)$ correspond to the maximum values of Artin’s constant, and the classes $R(8,i,x)$, $R(27,i,x)$ and $R(125,i,x)$ correspond to the minimum values. A simple analysis of each class shows that the dynamics of their formation has a rather complex nature, the analysis of which by analytical methods in the general case, if possible, requires the creation of complex methods. In our opinion, it is almost impossible to create a universal analytical method. The dynamics of $R(27,i,x)$ and $R(125,i,x)$ is significantly different from $R(8,i,x)$ despite the fact that the Artin’s constant takes the same values.

It can be concluded that in the processes of forming classes of prime numbers in the generalized and extended Artin's conjecture, for its improvement and deepening, it is necessary to have information about the laws of distribution of primitive roots, and in general, the indices of prime numbers.

Properties of the distribution of primitive roots of prime numbers

Thus, the equation of the Riemann zeta function in the Dedekind form under such circumstances is difficult to reasonably apply in methods of solving the problem at different values of *a* as a classifier of the set of primes. Therefore, it is necessary to create the basis of methods for analyzing the distribution of primitive roots and indices for prime numbers. Consider the algorithm for calculating $ind(a,p)$ for all *a* from an ordered set of integers associated with a prime *p*:

$$\{1,2,3,4,5,\cdots,n-1,n,n+1,\cdots,p-2,p-1\}=A_p$$

Let us define $ind(a,p)=(p-1)/card(a,p)$ where $card(a,p)$ is equal to the smallest *k* at which $a^k \equiv 1 \pmod{p}$. Obviously, if $k=p-1$ then $a^{p-1} \equiv 1 \pmod{p}$ and

$a^{(p-1)/p_i} \neq 1 \pmod p$, for any prime divisor p_i of the number $p-1$. In the case when $k < p-1$ then *k* always divides $p-1$ and $ind(a,p) > 1$, and if *a* is a primitive root, then $ind(a,p) = 1$. Suppose that *a* is a primitive root of a prime number *p*. Consider the basics of index theory in recursion:

$$x(0) = 1, \quad x(1) = a,$$
$$x(n+1) \equiv ax(n) \pmod p$$

44* MERGEFORMAT ()

and *n* changes up to $n = p-1 = \prod_{i=1}^{k} p_i^{\alpha_i}$. Let's calculate the Euler function $\varphi(p-1) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)$. The given function determines the number of numbers that are mutually prime to $p-1$. In recursion (1) in $x(n)$, the value *n* will be called the index, and the $x(n)$ is the residue modulo *p*. It is obvious that if *a* is a primitive root of *p* the index runs through all values from 1 to $p-1$. It is clear that between indices and residuals for each *a,* which is the primitive root of a given prime number *p*, there is a one-to-one correspondence with respect to p-1 and vice versa. Suppose that the set of all primitive roots is known:

$$\{a_1, a_2, a_3, \ldots, a_{\varphi(p-1)}\}$$

55* MERGEFORMAT ()

We will assume that if $a = a_1$, then $x(n)$ in (1) will run through all elements of the same set of values, but in a different sequence. In general, there is no simple algorithm for finding this sequence. Based on Euler's theorem of primitive roots, the following theorem holds.

Theorem 1. If in $x(n)$ index *n* is not divisible by any prime divisor $p-1 = \prod_{i=1}^{k} p_i^{\alpha_i}$, then residue $x(n) \equiv a_1$ is the primitive root of *p* [12]. The proof follows from Euler's theorem of primitive roots. It is obvious that in such cases *n* is a mutually prime number with and therefore in the recursion $x(n+1) \equiv ax(n) \pmod p$ such numbers, that is, the primitive roots will always be $\varphi(p-1)$. It follows that if in the sequence $x(n)$ *n* is divisible by the number *k* that divides $p-1$, then $x(n)$ is not a primitive root of *p* and this means that when $x(n) = a$ then $ind(a,p) > 1$. Thus, we find the largest value of *k*, at which this number divides *n* in $x(n)$. Then we assign $ind(a,p) = k$ and $card(a,p) = (p-1)/ind(a,p)$, and therefore $a^{(p-1)/k} \equiv 1 \pmod p$ is fair. Thus, the theorem is true.

Theorem 2. If in the sequence of $x(n)$ calculation is based on the primitive root and the index *n* is divisible by the maximum number *k*, then $ind(a,p) = k$ and $card(a,p) = (p-1)/k$. This theorem is true for any primitive root a_j of the set of all primitive roots $\{a_1, \ldots, a_j, \ldots, a_{\varphi(p-1)}\}$. Based on the above considerations, it is possible to formulate the theorem.

Theorem 3. In the set $\{1, 2, 3, \ldots, p-1\}$ for each primitive root a_i in the Fermat recursion (formula (3)) for any possible divisor *l* of $p-1$ there is a set of numbers $\{a_{l,1}, \ldots, a_{l,\varphi((p-1)/l)}\}$ which are the remainders of the recursion modulo *p* whose indices are $ind(a_{l,j}, p) = l$ and $(p-1)/l = card(a_{l,j}, p)$, and in the corresponding index system each of them is divided by *l* and *l* is their greatest divisor.

The validity of the theorem follows from the fact that all numbers of the set $\{a_{l,1}, a_{l,2}, \ldots, a_{l,\varphi((p-1)/l)}\}$ are mutually prime to $\varphi((p-1)/l)$ and are generating elements of the corresponding subgroups of the group of residues Fp^*.

Thus, we get the set of numbers *a,* for which $ind(a,p) = l$. It should be noted that in the above analysis it was assumed that the smallest primitive root was known. In the general case of choosing a set of consecutive primes $[p_n, p_{n+M}]$, the values p_n and *M* can be chosen to be large, and therefore the following calculations by computer modeling methods of the formation of classes

$F(a,i,x)$ and the calculation of constants $c(a,i,x)$ can be significantly complicated due to the fact that for each subsequent prime number it is necessary to find the smallest primitive root. In the absence of such information, finding the smallest primitive root can significantly complicate the calculation [15].

Thus, it can be concluded that $p-1=\prod_{i=1}^{k} p_i^{\alpha_i}$ actually defines a whole set of different divisors $\{l_1, l_2, \dots, l_v\}$. The values $l_1=1,\dots,l_v=p-1$ such that each l_j, based on theorem (3), defines $\varphi((p-1)/l_j)$ and $\{a_{1,j}, a_{2,j}, \dots, a_{\varphi((p-1)/l_j),j}\}$ is the set of mutually prime numbers such that $ind(a_j,p)=l_j$ and $card(a_{i,j},p)=(p-1)/l_j$. The law of distribution for each divisor l_j on the set $\{1,2,\dots,p-1\}$ unknown in the set of all $ind(a,p)$ for each *p* is still an unsolved mathematical problem. It is still possible to assume that such a law exists for all prime numbers *p*, but for numbers $p=4k+1$ the law of distribution of indices will differ significantly from the law of distribution for prime numbers of the type $p=4k+3$.

It should be noted that $ind(a,p)$ are divided into two classes of values *a*. In one class we will include those *a* for which $ind(a,p)=2l+1$, $l\in\{0,1,2,..\}$, and those *a* for which $ind(a,p)=2l$, $l\in\{0,1,2,..\}$ will be assigned to the second class. The case when $ind(a,p)=1$ belongs to the class $ind(a,p)=2l+1$ at $l=0$ is radically different from the case $ind(a,p)=2l$. It is generally accepted that if $ind(a,p)=2l$ then *a* is a quadratic residue, while if $ind(a,p)=2l+1$ then *a* is not a quadratic residue. The number of quadratic residues and nonquadratic residues is the same - $(p-1)/2$, but their distribution on the set $\{1,2,\dots,p-1\}$ is quite different. Consider the case $ind(a,p)=1$. Let us find the distribution of the primitive roots by the distance between them. It is easy to prove that the average distance between the primitive roots is defined by the expression $(p-1)/\varphi_i(p-1)$. The need to find such a law is primarily due to Artin's conjecture and the need to find numbers *a*, at which the structure of the class The term: the distribution of primitive roots of a prime number, should be considered from different points of view, and therefore the possibility of using probabilistic methods should not be excluded. Suppose that given a prime number *p* from the set $[p_n, p_{n+M}]$: $A_p=\{1,2,3,\dots,n-1,n,n+1,\dots,p-2,p-1\}$. A simple analysis of this set shows that at $a=1$ or $a=p-1$ then they cannot be the primitive roots based on the trivial reason: $card(1,p)=1$ and $card(p-1,p)\equiv 2 \pmod p$ for any *p*, and therefore $ind(a,p)=p-1$ and $ind(p-1,p)=(p-1)/2$ moreover, they are exclusive elements of a similar set for any other prime number. If we consider any other number *a* from this set, then it is quite difficult to estimate the probability that *a* is the primitive root of *p*, and its measure, with increasing value of *p*, grows exponentially.

Still, there are simple ideas for analyzing the laws of formation of such estimates. According to Euler's theory, the number of primitive roots of a prime number *p* is determined by the Euler function $\varphi(p-1)=\prod_{i=1}^{k_p} p_i^{\alpha_i-1}(p_i-1)$, so we can use the estimate $p(a=a_i(p))=\varphi(p-1)/((p-3)-k_p)$ where k_p is the number of squares in A_p, $\{1,p-1\}\notin A_p$. The distribution of primitives should give an estimate of the value of the smallest primitive root, in the literature there are attempts to obtain such estimates [11], but this is a rather difficult problem.

Since for each *p* the number of primitive roots is equal to $\varphi(p-1)$, the average distance between the primitive roots is $(p-1)/\varphi_i(p-1)$, provided that we consider cases where the smallest primitive root is not large. One of such properties can be considered the laws of distribution of distances between adjacent primitive roots and the laws of distribution of sets of primitive roots on intervals of a certain size. Consider a universal program for calculating all primitive roots of prime numbers of types $4k+1$ and $4k+3$ with different values of $\varphi(p-1)$ based on a universal algorithm for calculating their primitive roots. And for each prime number, the set of all primitive roots is partitioned into a system of ordered subsets, each of which includes primitive roots, the distance between which is sequentially $1,2,3,\ldots n\ldots$. At the same time, distribution laws for all types and classes of prime numbers were systematically studied. It was found that in all cases the mathematical form of the distribution law had the same form. Graphical analysis led to the conclusion that the distribution has an exponential form, the parameters of which depend on the properties of the corresponding prime numbers. It was proved that the distance *l* between the primitive roots has an exponential form of the probability distribution law:

$$f_p^q(\ )=\varphi\left(\frac{p-1}{q}\right)e^{-\lambda_{qp}(l-1)}$$

Where *q* is an index, then $\lambda_{qp}=f\left(\varphi\left(\frac{p-1}{q}\right)\right)$ constant for approximation of distribution classes number with distance *l* between them and index *l* for $p=4k+1$ & $p=4k+3$.

Let's consider an arbitrarily chosen system of consecutive eight primes:

p	*p decomposition*	$p-1$	$p-1$ factorization	$\varphi(p-1)$
2423	$4\cdot605+3$	2422	$2\cdot7\cdot173$	1032
2437	$4\cdot609+1$	2436	$2^2\cdot3\cdot7\cdot29$	672
2441	$4\cdot610+1$	2440	$2^3\cdot5\cdot61$	960
2447	$4\cdot611+3$	2446	$2\cdot1223$	1222
2459	$4\cdot614+3$	2458	$2\cdot1229$	1228
2467	$4\cdot616+3$	2466	$2\cdot3^2\cdot137$	816
2473	$4\cdot618+1$	2472	$2^3\cdot3\cdot103$	816
2477	$4\cdot619+1$	2476	$2^2\cdot619$	1236

Table 2. Structure of the prime factorization of $p-1$

The analysis of the prime numbers given for example shows that the formation of primitive roots and their distribution differ significantly even for consecutive prime numbers. The number of primitive roots varies widely enough, even though the difference between the given primes is insignificant. This elementary fact became the fundamental basis for the search of laws according to which the generalized Artin's constants take the same values over such sets of consecutive primes. If the value of *M* is fixed, provided that its value ensures the accuracy of the estimation, then it is important to find a mathematical justification for such stability of the obtained estimates [6,8]. In fact, the formation of classes $F(a,i,x)$ and constants $c(a,i,x)$ for all values $i=ind(a,p)$ can be interpreted as the process of designing a system of characteristics of prime numbers over the set $[p_n,p_{n+M}]$.

Distance	p=2423	p=2437	p=2441	p=2447	p=2459	p=2467	p=2473	p=2477
1	444	189	377	610	614	281	274	617
2	244	126	228	306	306	162	178	304
3	147	86	135	150	152	121	114	158
4	87	58	94	80	79	89	68	86
5	48	34	46	38	36	61	68	38
6	24	32	32	19	19	27	46	8
7	12	24	16	9	14	19	22	10

8	14	10	14	4	2	20	16	6
9	4	8	6	3	3	10	8	6
10	4	6	2	1	1	14	6	2
11	2	6	2	1	1	2	10	
12		2	6			5	2	
13		2				1	1	
14		2				1	2	
15		2				1		
16	1	2				1		

Table 3. Distribution of the distance between the primitive roots

The quality of the estimates of Artin's constants does not depend on p_n, but largely depends on the magnitude of *M* [8]. The distance between consecutive primitive roots of any prime number is distributed according to the exponential law. Mathematical justification of the exponential form of the probability law of distribution of the distance between the primitive roots of any prime numbers $p > 10^3$ is not simple. The correctness of this hypothesis follows from the fact that the processes of formation of the primitive roots are Poisson [16]. This statement is true because the formation of $ind(a, p)$ occurs under the influence of a significant number of factors that are independent of each other and the influence of each of them is insignificant, which leads to the formation of prime numbers, and therefore the theorem is true.

Theorem 4. For any prime number *p*, the set of primitive roots has the exponential form of the law in terms of the distance between consecutive primitive roots between them,

$$f_p(\ ) = \varphi\left(\frac{p-1}{q}\right)e^{-\lambda_p(\ +1)}$$

Note that the statistical estimation of the parameter λ_p will be correct only if the estimates of the values of all primitive roots of the prime number *p* are known, i.e., the set $\{a_1, a_2, \dots, a_{\varphi(p-1)}\}$. It can be argued that the "smoother" a prime number is, the smaller $\varphi(p-1)$ and, correspondingly, λ_p. Thus, if the measure of smoothness of a prime number p_k is greater than the measure of smoothness of a prime number p_{k+1} , then the inequality $\lambda_{p_k} < \lambda_{p_{k+1}}$ is true.

It is necessary to pay attention to one more important property of primitive roots, which is associated with the existence of internal cycles of primitive roots that arise in the processes of implementing a recursive function when moving to another primitive root of a chosen prime number *p*. It can be argued that the smoother the $p-1$ by λ_p less. Since the term "smooth number" still does not have a clear definition, in the number theory [12,13] the above results will be considered as an experimental fact that can be substantiated meaningfully, but a detailed mathematical analysis for the correct proof of all theorems related to the distribution of primitive roots and indices of any value, similar to the analysis given in the works of Erdős-Katz [14] and E. Kowalski [15], will be the subject of a separate work. Probabilistic proof of the exponential distribution law of $f_p(\ )$ will be the subject of a separate study, parallel to the study of the laws of distribution of not only the primitive roots, but also indices $ind(a, p) > 1$. This problem in number theory is quite complicated and there are no sufficiently deep results[13].

Deepening of the exponential law of distribution of distances between adjacent primitive roots is associated with another property of the distribution of primitive roots and indices, which is that for any set of consecutive primes $[p_n, p_{n+M}]$, provided that *M* is not less than a certain value (assumed $M=500000$), then there exists a number *Q* that for each prime number *p* from this interval, the set $1, 2, 3,\cdots..p-2, p-1$ is covered by a system of such intervals, where each interval contains the same number of primitive roots. This statement can be transferred to indices up to a certain value, which depends on the value of *M*. A deeper analysis of the theory of such coverage will be considered as a uniform law of distribution of primitive roots.

Conclusions

It is proved that the processes of formation of Artin’s constants of any integer *a* largely depend on the properties of not only the primitive roots of primes, but also on the properties of their indices for different primes. Neglecting the properties of indices generally leads to inaccuracies in their estimates. The justification of the necessity to have detailed information about the properties of classes of prime numbers with different values of indices of their elements and their structural properties is given. The exponential law of distribution of the distance between the primitive roots of any prime number *p* is found as a basis for studying the laws of distribution of their indices.

References

1. Crandall R., Pomerance C., Prime numbers. A computational perspective. Springer Science.
2. Rogers Jr. H. Theory of recursive functions and effective computability, Massachusetts Institute of Technology.McGraw-Hill Book Company, New York, 1987,673pp.
3. Manin Y., Panchishkin A. Introduction in modern number theory: fundamental problems, ideas and theories, Springer, 2005.
4. Kullback S. Information Theory and Statistics. Professional Lecturer in Statistics. The George Washington University. New York – John Wiley & Sons, Inc.London – Chapman & Hall, Limited. 1967, 408pp.
5. Shannon C.E. A mathematical theory of communication. Bell System Tech. Journal, 1948, Vol.27, 379-423; 623-656.
6. Shannon C. E. Communication in the presence of noise, Proc. IRE, Vol. 37, 1949, 10-21 pp.
7. Martin F.G. N., England J. W. Mathematical Theory of Entropy, Addison-Wesley Publishing Company. Advanced Book Program, Massachusets, 1981, 361pp.
8. Tomei A. Lawrence, Morris Robert, Encyclopedia of information technology. Cirriculum integration. Information science reference. Hershey, New York, 2008, 1045pp.
9. Black Jeremy, The Power of Knowledge. New Information and Technology Made the Modern World. Yale University Press, Now Haven and London< Copyrigt 2014>, 505pp.
10. Ricardo Baeza-Yates, Berthier Ribeiro-Neto, Moden Information Retrievel the concepts and technology behind search. Addison-Wesley publishing company, 2011,946pp.
11. Fox R., Information Technoloy. An Introduction for Today’s Digital World. CRC Press, A CHAPMAN&amp;HALL BOOK,2013, Taylor &amp;Francis Group, LLC, 556pp,
12. Artin E., The Collected papers. Addison-Wesley publishing company.INC 1965.
13. Hasse H., Uber die Artinische Vernutung und Verwandte Dichtefragen. Annales Academiae Scientiarum Fennicae, A. I. Math.-Phys, 116 (1952).
14. Bilharz H. Primitivisoren mit vorgegenbener Primitivwurzel, Math. Ann. 114 (1937) 476-492.
15. Vostrov G., Opiata R., Computer modeling of the processes of development of information technology in dynamic processes of the formation of classes of prime

numbers of the generalized Arin’s hypothesis. Monographs of National University Odessa Polytechnic. Ukraine, 2021,

16. Vostrov G., Opiata R., Probabilistic methods in computer simulations of the formation of classes of primes and estimations of the constant of the generalized Artin’s hypothesis. JMLR Workshop and Conference Proceedings 1:1-13, 2020, 9th Symposium on COPA.

17. Hooley Ch., On Artin’s conjecture. Journal fur die reine und angewandte Mathematics. Sonderabruck aus Band 225, 1967, Seite 209 bis 220.

18. Hooley Ch., Applications of sieve methods in the theory of numbers. Cambridge University Press. 1976.

19. Pomerance C., Rassias Th. M., Editors. Analytic Number Theory, Springer, 2015.

20. Murty Ram M., Problems in analytic Number Theory. Springer. 2008.

21. Lacasa L., Luque B., Gomes I., Miramontes O., On a Dynamical Approach to Some Prime Number Sequences. Entropy. MDPI.2021.

22. Vostrov G., Ponomarenko O., stochastic analysis of the smooth numbers’ properties and their search. International Conference –Computer Analysis and Data Modeling, Minsk, 2019.

23. Ambrose Ch. D. On Artin’s Primitive Root Conjecture. Georg-August-Universitat Gottingen. Geiidelberg. Dissertation 2014.

24. Tenenbaum G., Introduction to analytic and Probabilistic Number Theory. American Mathematical Society, 2015.

25. Granville A., Smooth numbers: computational number theory and beyond Algorithmic Number Theory MSRI Publications Volume 44, 2008

26. Kac M., Statistical the independence in probability, analysis and number theory, the carus Mathematical Monographs Number 12, JOHN WILEY and SONS, inc.1959

27. Kowalski E., Arithmetic Randonnee. An Introduction to probabilistic number theory. Versus of May,2021